GuIA.ai

Intellectual property rights and transparency of AI systems: an analysis from the Mexican legal system

Jorge Luis Ordelin Font

November 2021

CETyS | LATAM DIGITAL CENTRO DE POLÍTICA DIGITAL PARA AMÉRICA LATINA

In collaboration with: fAIr LAC | BID Banco Interamericano de Desenvolvimento

Intellectual property rights and transparency of AI systems: an analysis from the Mexican legal system

Author: Jorge Luis Ordelin Font

Coordinators: Carolina Aguerre y Maia Levy Daniel

Revision: Gonzalo Bustos Frati y Matías Jackson

Design: Mónica Castellanos

Translation: Verónica Penelas

Intellectual property rights and transparency of AI systems: an analysis from the Mexican legal system

November 2021

Jorge Luis Ordelin Font

Professor and consultant in intellectual property. Researcher of the Mexican National System of Researchers (SNI-1). Post-doctorate degree in Law (PNPD/CAPES), specializing in intellectual property. Facultad Meridional IMED, Brazil. Doctor in Juridical Sciences by the National Court of Scientific Degrees of the Republic of Cuba. Master's degree in Intellectual Property, Universidad Austral and WIPO. Master's degree in Civil Law, University of Havana, Cuba. Member of the Research Line on Law and Artificial Intelligence, Institute for Legal Research, Universidad Nacional Autónoma de México. (UNAM). Email:jlordelin@gmail.com

Executive Summary

One of the biggest challenges in artificial intelligence is to close or reduce the gap between transparency as an ethical aspiration of these systems and the national regulation of intellectual property rights. In this context, the objective of this paper is to analyze the legal framework of intellectual property rights for the protection of AI systems in accordance with the principle of transparency of these systems, taking the Mexican legal system as the object of analysis. Qualitative research methods were used for its creation. The relationship between intellectual property rights and the principle of transparency of a reliable AI system is explained from the theoretical legal analysis, while the content analysis of legal norms allows addressing this relationship in the Mexican legal system. The main conclusion reached is that intellectual property rights should not constitute a barrier to guarantee the materialization of the principle of transparency of artificial intelligence systems.

Contents

1. Introduction

From the legal and ethical standpoint, there are multiple debates on the international regulation of artificial intelligence (hereinafter AI) systems. At the international level, for example, Unesco has recognized that ethical values and principles are not legal standards, although they contribute to the harmonization of legal norms, their development and application, and provide guidance when the scope of these norms is unclear or when they have not been established due to the speed of technological development (2020). At the national level, legal standards of a diverse nature converge, ranging from the protection of fundamental rights (data protection, privacy, equality, etc.) to consumer protection and civil liability, among others. As the European Union has examined, it is necessary to analyze whether this heterogeneous and diffuse regulatory framework can cope with the risks posed by the use of this technology; in other words, whether it can be enforced or whether it needs to be adapted or created (European Commission, 2020).

One of the legal frameworks involved in the governance of these systems is intellectual property rights. These rights may or may not prevent the monopolization of AI, while, on the other hand, they impact on the fulfillment of the requirements for reliable AI. Intellectual property rights are exclusive rights that grant their holders a legal monopoly. The non-recognition of these systems as creations and/or inventions could discourage innovation in this technological field, while, on the other hand, excessive protection could be dysfunctional and also cause the same effect, which is discouraging innovation (Hilty, Hoffmann, Scheuerer, 2020). It is important to note that it is not only intellectual property norms that could lead to this reduction in incentives, since overly strict legislation in other areas could also have the same consequences[1]. In relation to intellectual property rights, the creation of monopolies over research, data, technology and the market impacts on the application and benefits of these rights in the solution of social problems by creating exclusions of use by rights-holders.

In principle, at least three major tensions can be identified that exist from the realm of intellectual property and governance of AI systems:

1. Existence of certification mechanisms for these viable systems and systems of intellectual property registries: is it possible to grant intellectual property protection when these systems are biased? What would be the value criterion or criteria for establishing protection criteria? Who would determine and apply them?
2. What is the relationship between the opacity and transparency of artificial intelligence systems and intellectual property rights?
3. Could one speak of a legal framework for the data used to train the AI system? Intellectual property or any other form of data protection could become a barrier to access these data, and thus to the knowledge that the use of this technology could provide.

1 V. gr. The establishment of disproportionate burdens on small and medium-sized companies, such as the certification of the systems generated by these.

This paper addresses the second of these tensions, i.e., the impact of intellectual property rights regulation on the opacity and transparency of artificial intelligence systems. The main working questions were the following: is the conception of a transparent artificial intelligence system contradictory to intellectual property norms? Are the legal provisions established in the Mexican legal system sufficient to guarantee the transparency of these systems and their balance with intellectual property norms?

The **objective** is to analyze the legal framework of intellectual property rights for the protection of AI systems in accordance with the principle of transparency of these systems, taking the Mexican legal system as the object of analysis. In accordance with this objective, the paper is divided into two main sections; the first section is aimed at explaining the relationship between the principle of transparency of a reliable AI system and intellectual property rights, including trade secrets as a protection mechanism, and, secondly, the way in which this relationship is addressed from the current regulation of the Mexican legal system. The relationship between transparency and property rights is approached from three fundamental perspectives: the way in which the types of protection of intellectual property rights can influence or affect the transparency regime of a system, under what assumptions or type of transparency it is necessary to access the protection provided by intellectual property rights, and the way in which this protection can be guaranteed during the different stages of the life cycle of the system, taking into account that transparency is not static but a process that must be guaranteed during all stages of the system's existence.

A qualitative methodology and research methods related to both Social and Legal Sciences, in particular the theoretical-legal analysis and the content analysis of legal standards, have been used for the creation of this document. The Mexican legal system is taken as a point of reference. Due to its technological development conditions in artificial intelligence, its legal system and its economic and social conditions, Mexico is a country that is of special interest as to the extent to which it is possible to advance or not in the design of strong and innovative AI systems.

As the main result, it is proposed to establish a relationship between the type or level of depth of transparency that must be guaranteed and access to information in AI systems that could be protected by intellectual property rights. The configuration of a harmonious system of protection and respect for intellectual property rights and the obligation of transparency are based on the type of protection of these systems, as well as on the regulatory and contractual provisions that exist around them. Intellectual property rights should not be a barrier to evaluating the algorithms, data use and design processes of AI systems.

2. Transparency as a principle for strong AI

The conception of reliable AI rests on three substantial components: 1) it must be lawful in a way that ensures respect for fundamental rights, existing laws and essential principles and values, 2) it must be ethical, by enabling the guarantee of an "ethical purpose", and 3) it must be robust, both from a technical and social point of view (European Commission, 2019, p. 6). Among the principles for the responsible design and use of AI systems, also called Fast Track Principles (FTP), are fairness, accountability, sustainability and transparency, all closely interrelated.

In particular, the term transparency relates to multiple concepts and serves many functions. Despite the importance of this principle for the management of AI systems, its scope and the way in which it is implemented is not always clear. There is usually confusion as to its meaning and scope. The complexity lies both in the concept, what to understand by transparency, and in the object on which it is based. There is no doubt that the latter determines the former as a complex, integrating, relational and non-static process, in which there are differences between the normative ideal and its practical application.

The transparency of the system is associated with the possibility that it can be easily observed and understood (Oliver, 2018). Not only in relation to the data that the system uses, but also, the way in which it works and the right of people to know that they are interacting with artificial systems. In other words, knowing how the data is collected, the needs of the data based on the algorithm, the sources from which data come, how the system is fed, its continuum of improvement and self-adjustment (Qiang, 2018, p. 22).

In the words of Hamon, Junklewitz and Sanchez, it is nothing more than "the documentation of the AI processing chain, including the technical principles of the model and the description of the data used for the conception of the model, including any element that provides a good understanding of the model and is related to its interpretability and explainability" (2020, p. 2). According to the OECD, a system is transparent if it provides meaningful information, appropriate to the context and consistent with the state of the art; if parties are aware of their interaction with it, including the workplace; if it enables those affected by an AI system to understand the outcome; and those adversely affected by its use to challenge its outcome based on easily understood information, particularly in relation to the factors and logic that served as the basis for the prediction, recommendation or decision (2019).

However, the truth is that the practical applicability of these concepts is much more complex than the conceptualizations outlined above. According to Felzmann et al., this causes a gap between aspiration and reality, driven partly by the broad and diffuse conception of the term and partly by the intrinsic complexity of the object of transparency, the algorithm. Therefore, its conception cannot be limited only to the transfer of information from one agent to another, but it is essential to pay attention to the meanings, values and social functions associated with it; in other words, to the normative and social character that underlies the concept (Felzmann *et al*., 2020).

According to Felzmann *et al*. (2020), it is necessary to integrate three perspectives of transparency in order to understand its role in AI systems. A normative perspective, a relational one and finally a systemic one. The normative notion assesses the behavior of agents, systems or organizations, their operations, intentions or considerations. Although this perspective is important, it does not specify the addressee or the audience to which an actor must be transparent, although the relational perspective does specify it since the analysis is carried out not from an individual characteristic but from the relationship that exists between the agent and the receiver, the way in which the addressee receives and understands the information. The design and assessment of the measure is carried out taking into account the impact on stakeholders. Finally, the systemic perspective takes into account the institutional context of transparency relationships, i.e. associated legal, regulatory and organizational measures. This context is essential for a realistic understanding of the probable practical impact and effective implementation, including the role and effectiveness of accountability.

The "ought to be" of a reliable AI system takes into account, among other criteria, the explainability of the system, the quality and intent of the process, its results and the way in which these are produced (European Commission, 2019, p. 6). It is closely related to trust, autonomy, a higher level of control and accountability. Lack of transparency constitutes one of the main risks that need to be addressed in the development of this technology, especially in terms of minimizing the chances that pre-existing biases and errors will be replicated, reinforced and prolonged by the use of this technology. All of which could translate into behavioral manipulation, dishonest use, labor displacement and technology appropriation, among others (Herrera, 2019, p.15).

Transparency is a cornerstone of system governance and in particular of its trust; it is part of the significant set of safeguards that must be adopted to make humans the center of algorithmic decision making. Depending on its practical implementation and the information obtained, people can continue to use or stop using information systems while at the same time contributing to increasing consumer trust and loyalty. However, this does not mean that transparency alone guarantees the system's effectiveness and accuracy. Other factors such as user expectations, transparency implementation, technologies, individual factors and cultural context need to be taken into account to achieve such trust (Felzmann *et al*., 2020).

There is a direct relationship between transparency, system explainability, governance of algorithmic accountability, algorithmic audit processes and algorithmic impact assessments. A transparent AI system also enables the attribution of responsibility and the consequences of its use in accordance with the role of each of the actors, the context and the state of development of the technology. Risk and harm are not associated with intentionality or guilt from an objective system since, even if there is no intention to cause harm, these may be present. Hence, transparency plays an important role in the identification and management of risks.

Although they are intrinsically related, the transparency associated with personal data cannot be confused with that of the system. The latter, also known as systemic transparency, goes deeper than the individualized transparency regime that applies to the holder of the personal data. Transparency associated with the quality of information about the system cannot be analyzed only in relation to the protection of personal data, but in relation to the functioning of the system itself. Although this interrelation is indissoluble, it is important to delimit it in order to be able to have clarity in relation to the responsibility of the system. Individual transparency

is not sufficient, especially in relation to the construction of the algorithm or its continuous performance. In the first case, transparency operates after the algorithmic development when the responsibility or correction of the system is more complex, being continuous and implemented from the first stage of algorithm development.

Transparency associated with the protection of personal data is determined by the fact that data holders are aware of its use, expressly authorize said use, know the cases in which the initially intended purposes are modified, but also when they are aware of the processes of dissociation of information, preservation of their identity, risk possibilities, reversal of the anonymization procedure or submission to a pseudonymization process, etc.

3. Transparency of AI systems and intellectual property rights: in search of a balance

The relationship between intellectual property rights and the transparency of AI systems constitutes one of the most complex overlapping scenarios between AI and intellectual property. As has been argued, the latter could create barriers and pose a conflict of norms between intellectual property protection and the societal need for transparency and accountability (Castets-Renard, 2020).

The opinion formulated by the Internal Market and Consumer Protection Committee of the European Parliament of July 9, 2020, recognized the need to reconcile intellectual property rights, including trade secrets, with the implementation of other public policy objectives such as respect for fundamental rights and freedoms (paragraph 4). Similarly, the European Commission's expert group that developed the ethical guidelines for reliable AI recognized the impact of intellectual property rights on the realization of the principle of fairness and respect for proportionality between competing interests and objectives. Said group pointed out that proportionality between the user and the deployer starts from taking into account the intellectual property rights of companies and the rights of users (European Commission, 2019, p. 15).

Ensuring transparency standards depends to a large extent on a collaborative governance framework, in the sense not only of the ability of the system to perform as expected or promised but also assuming that the different actors are willing to disclose such information (Felzmann *et al*., 2020). For Felzmann *et al*., it is necessary to transmit knowledge, documentation and timely instructions at any stage of the transparency process; only in this way is it possible to ensure that the various actors in the life cycle of the system are committed to its transparency and are accountable for the role they play. However, we cannot be unaware that intellectual property rights may limit the exercise of this transmission of information and documentation, depending on the owners and the forms of protection that have been used.

Intellectual property rights have a direct effect on the so-called intentional opacity of AI systems. This type of opacity has also been referred to as private access barriers (Felzmann *et al.*, 2020), allowing third parties to be deliberately excluded from access to the AI system software and algorithm in order to protect the ownership of the former as well as to maintain the commercial and competitive value of the AI system in the market. Intentional opacity or opacity to protect ownership or corporate secrecy is related to other forms of opacity, knowledge and intrinsic opacity, in conjunction with which it must be analyzed, the latter being determined by the complexity of the system and its interpretability[2].

As systems become more complex, they can process a greater amount of data and at the same time are more difficult to interpret. (Oliver, 2018, p. 26). Technical limitations are linked to the

2 Burrell speaks of three forms of opacity, "(1) opacity as self-protection and intentional corporate or institutional concealment, i.e. the possibility of conscious deception; (2) opacity derived from the current situation in which writing (and reading) code is a specialized skill and; (3) an opacity arising from the mismatch between mathematical optimization in the high dimensionality feature of machine learning and the demands of human-scale reasoning and semantic interpretation styles." (2016).

autonomous, complex, and scalable nature of AI. The algorithms and code are highly technical and complex. It is not just the ability to read code, which in itself is already a specialized skill not found in the general public. The models that are useful for their accuracy are becoming more and more complex, and this seems to be inevitable. Thus, it will become increasingly common that system understanding and interpretation can escape human comprehension, even for those with specialized knowledge; there is a mismatch between the mathematical procedures of machine learning algorithms and human styles of interpretation.

Each of these forms of opacity will have to be addressed from different strategies, tools and approaches ranging from legislative to organizational or programmatic and technical. It is necessary to identify the type in order to mitigate it according to a determined action plan in which technical and non-technical solutions converge, of dissimilar nature, such as regulatory aspects, types of audits, and more transparent alternatives such as open source, public education, and programmer awareness, among others. Therefore, given that this work deals particularly with the so-called intentional opacity or the opacity that arises from the protection of property or corporate secrecy, it is important to understand the limits of the proposal analyzed in this work. This does not imply that it can meet the demands of transparency on its own; it is part of a more complex problem and, therefore, constitutes a part of the solution, but not the only one.

Finding a balance between these systems is neither easy nor simple to solve. For some authors, such as Oliver, this type of opacity can be mitigated through the use of open software; however, the existence of economic and commercial interests in these types of development cannot be ignored, and therefore, although desirable, it is not possible to aspire to this being the type of protection that would be used in all cases.

In this sense, the proposed EU regulation requires that the obligation of transparency does not disproportionately affect the right to intellectual property protection. It could be said that it implicitly recognizes an impairment or at least an impact. Likewise, it recognizes industrial and commercial property as an exception to the conformity assessment, together with public safety, protection of life and health of natural persons. Although the assumptions under which it would operate are not clearly established, its exceptionality is clear by taking into account the rapid availability of innovative technologies, their impact on health, the safety of individuals and society as a whole (recital 68).

For Castets-Renard (2020), meeting the objectives of transparency and accountability does not concern the algorithmic rules but the results and the explanation of their application. Thus, the author believes there is no risk of infringement of intellectual property rights and trade secrets; these rights should not be used to prevent the disclosure and explanation of artificial intelligence systems. However, as we will have the opportunity to analyze, there is a tension between them, but it does not materialize in the same way since it depends on the levels of transparency required.

Transparency is related to the ability of a third party to examine the system to ensure certain standards in decision-making, verifiability or traceability of the system. Access to the algorithm makes it possible to establish the relationship between the system and the results of its application (Eticas Research and Consulting SL., 2021), but it will not be necessary to guarantee

such access in all cases since this depends on the levels of transparency. The question to be answered is how much transparency is necessary to meet the "ideal" of a reliable system and the expectations of the parties (Hamon, R., Junklewitz, H., Sanchez, I., 2020). Much is made of the need to take into account both the context in which it takes place, the stage of the system life cycle and the recipients. However, it should be kept in mind that too much transparency could also bring harmful and unintended effects. As Felzmann et al. state, it is not clear that higher levels of transparency are always best. Ideally, an optimal level of transparency would be one in which "the desired and achieved transparency coincides with the respective person or group" (2020, p. 3354). However, from a practical point of view, achieving a balance between different perspectives, positions and interests is not always easy to accomplish. The actors in the system vary depending on their life cycle and with it also the various interests that are manifested in relation to the system.

From the perspective of intellectual property rights, greater transparency could lead to the loss of the exclusivity involved in the exercise of rights over creation and the consequent loss of competitive advantage (Burell, 2016). It should not be forgotten that algorithms as technical and mathematical elements that are located in a given business model are applied to a specific group of users and seek profits or a form of profit. They not only collect data from people; their results are also applied to them.

3.1. Levels of transparency and intellectual property rights

Transparency is undoubtedly related to the depth of the information that is disclosed and the time at which this disclosure takes place. In this sense, there are different levels or visions of transparency because its content varies depending on its nature and context. Pasquale, quoted by Kaminski (2019), uses the term "qualified transparency", which defines a system of specific disclosures of different degrees of depth and scope that varies according to the intended recipient. The assumption is that disclosures are different types, whether they are directed to the public, to the internal of the company, to regulators or to third parties. For Kaminski (2019), some of these subjects should have access to the source code and others should not.

The "qualified transparency" or the reference to "some degree of transparency" would seem to be a way of balancing the transparency requirements of the systems with the limitations posed by their intentional opacity. However, referring to an "adequate level of transparency" is not an easy matter. Especially if we take into account that this level depends not only on the information that needs to be transmitted and the way in which the system is protected, but also on other factors such as the complexity of the algorithm, type of opacity, target audience, context, expectations and information that needs to be transmitted in order to satisfy them, among others.

A possible solution could be found in the community proposal, which is based on the distinction between: 1) the minimum information necessary for individuals to exercise their right to an effective understanding and, 2) the transparency necessary for supervisory and law enforcement activities.

a. Adequate level of transparency in relation to users

This level of transparency starts from a perspective that could be called individual in that the information must not only be disclosed, but also received, interpreted and understood by the receiver and according to their needs. Referring to the obligation of transparency from this logic, Kaminski (2019) says that, although it is not necessary to provide the source code to people, a description of how the algorithmic system works in decision making must be provided, i.e., it is not necessary to transmit information about the algorithm per se but about its use and results. Compliance with the principle of transparency would not, in principle, imply an infringement of the protection afforded by intellectual property rights. The adequacy of the information is determined by how understandable, meaningful and actionable the information is rather than by whether or not one has access to the source code and other information associated with it.

In this sense, Article 13 of the proposed European Community Regulation refers to a level of "sufficient transparency" for users to correctly interpret and use their output information. Compliance with this standard is complex, especially because, in addition to the person or group of persons to whom the information is addressed, it must be taken into account that the interpretation and understanding of the information as an intellectual activity depends on several factors[3]. How much information needs to be provided is complex to delimit. To this effect, the aforementioned article refers in paragraph 3 to the minimum content of information that must be made known to the user in order to comply with the transparency obligations of high-risk systems[4].

Delimitations such as the above are important to adopt not only to guarantee the minimum content of transparency, but also because at the same time they become a limit to the information that may or may not be protected as confidential or trade secret. In this way, only information that does not fall within this content will be considered confidential.

At the user level, the principle of transparency is marked by the need for the information transmitted to be understandable or legible to all. The transmission of information related to the systems is required to be clear and concise, in particular that related to risks to fundamental rights and discrimination. For example, according to the proposed European regulation, it is necessary to accompany the instructions for use, in digital or other appropriate format, with "concise, complete, correct and clear information that is relevant, accessible and understandable to users" (art. 13.2).

It should be kept in mind that if information is presented in a complex and obscure manner, it does not imply greater autonomy and control on the part of the user, nor does it imply

3 Among which may be mentioned the digital skills of the person, his or her capacity for understanding, as well as the educational, cultural and economic context in which he or she lives.

4 These include: a) identity and contact details of the provider and, where applicable, of his authorized representative; b) the characteristics, capabilities and limitations of operation of the high-risk AI system, and in particular: (i) its intended purpose; (ii) the level of accuracy, robustness and cybersecurity against which the high-risk AI system has been tested and validated and can be expected to perform, as well as any known or foreseeable circumstances that could affect the expected level of accuracy, robustness and cybersecurity; (iii) any known or foreseeable circumstances that could affect the expected level of accuracy, robustness and cybersecurity; (iii)any known or foreseeable circumstances, associated with the use of the high-risk AI system in accordance with its intended purpose or reasonably foreseeable misuse, that could give rise to risks to health and safety or fundamental rights; (iv) its performance in relation to the persons or groups of persons in relation to whom the system is intended to be used; (v) where applicable, specifications regarding the input data, or any other relevant information regarding the training, validation and test data sets used, taking into account the intended purpose of the AI system; (c) changes to the AI system and its performance predetermined by the supplier at the time of the initial conformity assessment, if any; d) the human surveillance measures, including techniques established to facilitate the interpretation of AI system output information by users; e) the expected lifetime of the high-risk AI system, as well as the maintenance and care measures necessary to ensure the proper functioning of the AI system, including with regard to software updates; f) the expected lifetime of the high-risk AI system, as well as the maintenance and care measures necessary to ensure the proper functioning of the AI system, including with regard to software updates.

compliance with transparency requirements but rather affects people's understanding of communication and makes the user responsible even when the information does not make sense. There is the potential for companies to inundate people with useless and unnecessary information, and it is even possible to create obscurity by means of information overload. For example, using something similar to the terms and conditions of digital services and licenses that are nowadays established in reality has proven to be inoperative (AEPD, 2018 and Hidalgo Pérez, 2020). The complexity of the terms and conditions demands a technical and legal knowledge superior to that of the average citizen, and have turned them into a mere formality while becoming at the same time ineffective, at least in terms of the objectives pursued, in particular, its understanding.

b. Adequate level of transparency in relation to the activities of supervision and certification of AI systems

In order to be able to perform oversight and certification activities of AI systems, another level of depth is required in access to system information and transparency. Audits and oversight of AI systems are beginning to be seen as part of the governance of organizations that design and implement AI systems. When conducted with an ethical approach, they contribute to strengthening the ethical infrastructure of mature information societies (Mökander and Floridi, 2021).

A complete view of the system is required when certification or monitoring of the system is performed, whether this is done in the design, implementation or evaluation process. Under this assumption, Hamon, Junklewitz and Sanchez (2020) point out three levels of transparency: in the implementation, in the specifications and in the interpretability. The first level referred to is standard and makes it possible to see the way in which the model acts on the input data to generate a prediction, the technical principles of the model and the associated parameters. The second refers to all the information related to the implementation, the model specifications, training data, procedure, performances, as well as any other element that allows to reproduce the implementation. The third and last level is related to the understanding of the underlying mechanisms of the model, such as the logical principles behind data processing and verification that the algorithm follows the specifications and aligns with human values.

Impact assessments, self-audits or audits by independent third parties, as well as control and supervision by regulatory authorities require deeper levels of transparency and greater information flows, including the source code. Therefore, access to information about the algorithms is necessary, which includes not only the algorithm itself but also all the information generated around it, including interpretative documents. It is important to note that access to this information does not depend on the complexity of the algorithm but on the purpose of the audit and supervision. Even if the algorithm is technologically obscure, access to this type of information may be necessary to analyze and correct its errors, inaccuracies, and biases.

It can be concluded that there are two sides to transparency; one is determined by the individual scope of the user or person using the system, its final recipient, and the other takes as its starting point the explainability of the system, the techniques used, its technical complexity and internal structure. Only in the latter case is it possible to refer to access to the source code

and information that could be protected as a trade secret or by another type of intellectual property right. However, the greatest challenge in the latter case is to guarantee said access to all the actors involved in the life cycle of the system, whether they are interested in its design, risk management, commercialization, distribution or even in determining legal liability.

4. Transparency and intellectual property rights in Mexico

In the relationship between the principle of transparency and intellectual property rights, one of the main contradictions that exist is between the territorial nature of intellectual property and the global nature of technology. Therefore, the study of this relationship must start from particular legal systems in order to bridge the gap between transparency as a principle and ethical aspiration of the governance of AI systems and the national regulation of intellectual property rights and other applicable regulatory regimes.

Under this premise, Mexico becomes a country of particular importance for the study of this relationship in the Latin American region, both from the point of view of technology development and the legal regulation of this matter. This makes the country a study model for the region in which it is possible to determine the impact of intellectual property regimes on the development and progress of artificial intelligence in general, and in particular on the materialization of the principle of transparency.

According to the index prepared by The Economist Intelligence Unit (EIU) and the company ABB in 2018, among the 25 countries prepared for the wave of intelligent automation Mexico ranks 23rd, after Argentina (17), Brazil (19) and Colombia (20). It also ranks 55th out of 172 in the 2020 AI government readiness index, according to the study conducted by Oxford Insights and the International Development Research Center (IDRC). This ranking measures how governments make responsible use of AI; one of the dimensions measured is precisely transparency in conjunction with accountability, privacy and inclusiveness.

In Mexico there are important studies by organizations and members of civil society for the development of an AI strategy. The document AI Strategy in Mexico: Harnessing the AI Revolution (British Embassy in Mexico, 2018, p. 8, hereinafter AI Strategy) recommended the modernization of intellectual property and privacy protection regulations in conjunction with investment in infrastructure that supports technology, good quality data and internet connectivity. Likewise, there is the Mexican National Agenda for Artificial Intelligence by the IA2030Mx Coalition, which offers a set of recommendations in this regard, including the implementation of public policies that promote the obtaining of patents and commercially viable products from developments in academia (2020, p. 43).

At the regulatory level, the entry into force of the Free Trade Agreement between Mexico, the United States and Canada (T-MEC) entailed the adoption of a new Federal Law for the Protection of Industrial Property (LPI), as well as important amendments to the Federal Copyright Law (LFDA). These modifications have undoubtedly led to the introduction of new legal concepts that have an impact on the protection regime of AI systems. These legislations offer a favorable regulatory framework for analyzing the relationship established between intellectual property rights and compliance with the principle of transparency in AI systems in the Mexican legal system.

4.1. How can intellectual property rights affect the transparency of AI systems?

The fundamentals of protection of intellectual property rights and transparency of AI systems differ. Transparency is not only related to the technical characteristics of the algorithm but also to its practical implementation within existing social structures and their assigned cultural meanings (Felzmann et al., 2020). To achieve it, it is necessary to understand the logic of the system and its limitations, in other words, the algorithm operating with data in a given context and circumstances. It is based on the protection of personal interests and the protection of individuals from the use of technology.

The recognition of intellectual property rights over these systems and the protection of secrets has a strong commercial character. As recognized in the TMEC, they provide effective protection against unfair competition in accordance with Article 10bis of the Paris Convention. Their use prevents their disclosure, acquisition or use by other persons without the consent of their owner and in a manner contrary to honest commercial practices (art. 20.70 TMEC).

Maintaining this distinction in terms of the purposes of each of the systems is important; however, this does not mean ignoring the role of intellectual property not only as an incentive for the promotion of this technology but also to guarantee its owners their rights against misappropriation and counterfeiting. These are risks that are also run with the introduction of certain products using artificial intelligence systems.

In order to determine the way in which intellectual property rights may affect the transparency of the system, it is necessary to understand the protection mechanism used and its scope. In principle, the algorithm as a defined sequence of steps used to solve a problem or obtain a result (art. 19.1 TMEC) is considered inappropriate, as Plaza Penadés states; however, in practice at least three possibilities of protection are identified based on their suitability for each of these concepts: trade secret, copyright (software) and by means of patents. All three scenarios constitute forms of exercising a legal monopoly.

In fact, an interesting aspect of the TMEC is the consideration in footnote 80 of chapter 20 as an object of misappropriation of computer systems. This implies subjecting them to the system of enforcement and protection of trade secrets in both civil and criminal law, provided that their acquisition, use or disclosure of the information is contrary to honest commercial practices, or the person or third party knew or had reason to know that such acquisition was contrary to such practices. Consequently, the computer program could be considered as the object of misappropriation as long as it meets the requirements to be protected as secret, i.e., being undisclosed know-how and commercial information, having commercial or real value precisely because it is secret, and being subject to reasonable measures according to the circumstances by whoever has its legal control[5].

One of the greatest risks of this form of protection and its impact on transparency is the fact that confidentiality contracts or clauses related to them become widespread, since it is the owner of the secret who determines its commercial value without there being any way of verifying whether it has such value. In fact, there may be a proliferation of information considered as

5 After the approval of the New Industrial Property Law in the Mexican legal system, this concept is regulated including the requirements for its application and interpretation. These requirements coincide with what is established in article 20.73 of the TMEC.

such that does not comply with the legal requirements set forth in the law, and in particular those for which sufficient means or systems have not been adopted to preserve confidentiality and restricted access[6].

The other form of protection of these systems is through patents. Mexico's AI Strategy states that a future reform of intellectual property law should recognize intellectual property rights for emerging technologies, allowing the protection of AI programs by patents and "not only that physical products can be patented" (2018, p. 46). Beyond the fact that there is a false assertion, given that not only physical products are patented[7], the fact is that after the adoption of a new industrial property law this concept was not introduced. Said law establishes that the following are not considered inventions: 1) mathematical methods; 2) schemes, plans, rules and methods for the exercise of intellectual activities, for games or for economic-commercial activities or for conducting business; 3) computer programs (art. 47). Although algorithms and computer programs are excluded from patentable subject matter per se, this does not prevent a product or process from being considered novel precisely because of the implementation of an algorithm. In fact, worldwide, data show that there has been a substantial increase in the protection of these systems through the use of patents as protection mechanisms[8].

The patent system presents some limitations that could impact the protection of these systems and their transparency, particularly in those that are opaque due to the will of their holders. The procedures to obtain a patent are not only lengthy procedures, which can go against the rapid development of technology, but also the patent claim does not show the system or algorithm itself; therefore, it does not contribute to the transparency of the system, at least in the terms to which we have been referring.

Patenting guarantees, in principle, transparency with respect to human inventiveness, not with respect to the AI system. According to Früh (2019), patent laws make it clear that the invention must work; therefore, the inventor does not have to know why something works. It is only necessary that it works; the disclosure requirement is not an issue. Disclosure of the AI technique should be sufficient. In fact, the invention can be known and patented even if the exact AI method is not disclosed. Generally, the assertion is elaborated from phrases such as "A computer-implemented system that facilitates and performs ...", "A computer-readable medium comprising computer-executable instructions for...", among others, which logically brings implications in the area of transparency and auditing of the system. In fact, the disclosure of the invention by means of a patent does not describe it explicitly.

From the patent system, transparency is not defined by whether the AI system is transparent or not, whether it is explainable or not, but by the balance of disclosure: "What information must the applicant disclose to the patent office so that the public understands what it is getting in exchange for the grant of monopoly rights?" (Früh, 2019, p. 15). This does not mean that

6 Although this legal concept allows a stronger protection than that of software, and faster than that of patents, it cannot be ignored that this does not prevent third parties from using the AI system in a lawful way as long as it is obtained by their own means. Nor does it guarantee protection against information that is obtained by reverse engineering, or independently or legitimately by persons who are under no obligation of confidentiality or simply have no knowledge that this information was secret and was not obtained in violation of honest commercial practices. In such cases, it is not possible to allege breach of contract or inducement of breach.

7 The subject matter of the patent is an invention, which may be a product or a process. As recognized in the IPL, this also includes the patentability of substances, compounds or compositions.

8 According to the 2019 WIPO report on this technology, since the 1950s more than 340,000 patents have been filed globally for AI-related inventions and more than 1.6 million scientific publications have been published in this regard, with more than half of these figures being from 2013 onwards. Applications related to machine learning have experienced an average annual growth of 28% (WIPO, 2019, p. 7).

the technology must be understood. Therefore, it is possible that the holder of an AI system is protected by a patent and this is not transparent since he is not under the obligation to submit it to a transparency process to ensure such protection. On the contrary, the exclusivity granted by this title allows excluding third parties from using and accessing the information held by the holder because the patent system does not condition to provide this information.

However, even if it is not necessary to know how the system works and what relationships are established in order to achieve patent protection, it must be reproducible. In principle, AI systems should be reproducible, but this is not always the case. It should be borne in mind that this may be due both to technological limitations of the system itself and to the data that are used to train it. Some of these inventions cannot be disclosed through the patent title without the additional disclosure of the data set used in its training, something that companies may not be willing to do. It is also possible that the evolution of the algorithm over time makes clear differences between the initially granted title and the one applied to a given product or service.

The impossibility of reproducing these systems not only impacts on their transparency, from the point of view analyzed in this work, but also on the very foundations of the patent system. According to Frühlas (2019), the disclosure deficit of algorithms lacking reproducibility requires rethinking the disclosure requirements of patent law by AI systems, in particular regarding the reproduction of the desired technical solution. In principle, the complexity of the AI system and its use should not increase this deficit.

Another form of protection of the AI system is as software by means of copyright. Reference is typically made to software-based AI systems, in which at their core is a software[9]. As already mentioned, the algorithm itself is not subject to protection, at least from the perspective of the Mexican legal system[10]. However, if said algorithm is converted into a programming language, its protection would be possible within the regulatory framework of the LFDA, specifically that which is recognized for computer programs and databases as provided for in sections XI and XIV of article 13 of the LFDA.

This means that the AI system can be protected if it complies with the requirements established by the norm and grants it certain exclusive powers that prevent its use by third parties not authorized by its owner. From the first meaning, the AI system must be considered as "the original expression in any form, language or code of a set of instructions that, with a determined sequence, structure and organization, is intended for a computer or device to perform a specific task or function" (art. 101 LFDA). It is protected on the same terms as literary works and includes both operating programs and applications, whether in the form of source code or object code (art. 102 LFDA).

Protecting the AI system as software, under the legal regime of copyrights, also implies recognizing the power of disposition of its owner over it that excludes third parties, which materializes in a set of moral and patrimonial faculties. Among the latter, the Mexican legal system recognizes the power to authorize or prohibit: (a) the permanent or temporary reproduction of the program in whole or in part, by any means and in any form; (b) the translation, adaptation, arrangement or any other modification of a program and the reproduction of the resulting

9 Some conceptions of AI are based on this concept to explain it, as is the case, for example, of article 3.1 of the proposed EU Regulation, which states that its objectives include contents, predictions, recommendations or decisions that influence the environment, which are defined by human beings.

10 Ideas in themselves, formulas, solutions, concepts, methods, systems, principles, discoveries, processes and inventions of any kind, as well as schemes, plans or rules for mental acts, games or business, among others, are not subject to protection (art. 14 paragraphs 1 and III LFDA).

program; (c) any form of distribution of the program or a copy thereof, including rental; d) the adaptation, arrangement or modification of the program, as well as the reproduction of the resulting program, the decompilation, the processes to reverse engineer a computer program and disassembly, e) as well as the public communication of the program, including the making available to the public thereof (art. 106 LFDA).

These powers guarantee the control of the owner of the software, its proprietary nature, as well as the access that they may or may not grant to third parties to the source code. This access in many cases depends on whether only the use of one or some of these faculties or the assignment of these faculties has been authorized. It is important to note that, although these powers make it possible to deprive access to the source code as part of the rights-holders' power of disposal, the fact is that the recognition of these powers is not contradictory to the so-called open software, a model that is advocated in favor of a transparent regime of AI systems as an alternative to the proprietary model that does not grant such access.

One aspect that deserves to be emphasized is that the above-mentioned forms of protection are not mutually exclusive; in fact, two or all three may exist on the same AI system. In this way it is attempted, as far as possible, to combine the benefits and disadvantages of each form of protection with the other, as long as the system complies with the requirements that each particular form demands. Undoubtedly, on the one hand, while guaranteeing the effectiveness of the system's protection and the lower probability of appropriation by third parties, on the other hand, the biases that each of these forms represent in relation to transparency also have an impact on the management of the AI system's transparency.

Intellectual property rights generally prevent the public availability of the implementation and specifications. However, this does not mean that there are no possibilities for making the demands of protection of intellectual property rights and transparency requirements compatible. Both in the case of patent protection and trade secret protection, there are exceptions that may be applicable although it is more difficult in the case of software, where the rules do not provide for express possibilities of making oversight mechanisms compatible with access to the source code.

In the Mexican system, for example, the industrial property law does not consider that the information related to the secret enters the public domain or is disclosed when it is provided to the authorities for the purpose of obtaining licenses, permits, authorizations, registrations or any other acts of authority (art. 163.1 IPL), such as the existence of a certification regime (art. 163.1 IPL)[11]. A similar provision is found in article 168 of the Mexican Industrial Property Law, which provides that, when it is mandatory to provide information considered secret to determine the safety and efficacy of pharmachemical or agrochemical products that use new components, this information would be protected under the terms of the applicable legislation or, as the case may be, of international treaties (art. 168 IPL). Even though this provision is not expressly applicable to AI systems, it could be modified or applied analogically to this case.

11 There is a broad international debate on the existence or not of certification mechanisms for AI systems, and under what assumptions they should be applied. In principle, there is talk of establishing certification mechanisms depending on the impact on people's lives and risks that should evaluate the impact of these systems, carry out follow-up audits and ethical and regulatory compliance. However, there are doubts as to how these certification mechanisms would operate, which must guarantee trust and legal certainty and, at the same time, not become an obstacle to innovation and the development of small and medium-sized enterprises. The proposals range from the conformity assessment proposed by the European Regulation, certification according to the different audit levels of the German Data Ethics Committee, the Danish data ethics seal or the Maltese voluntary certification system. In Mexico, the establishment of a Mexican AI ethics council composed of experts, business leaders and the AI Office is being discussed in order to a) establish guidelines and limits that reflect Mexican values and b) grant a seal of quality to AI companies that respect the standards (British Embassy, 2018).

In patent matters, for example, the registry is public with the exception of confidential applications (art. 22 IPL). Thus, the files could not be open to consultation and promotion if they contain information of this type (art. 23 IPL), and could be consulted by the applicant, their legal representative or by persons authorized by said applicant. The observance of the preservation of confidentiality implies the administrative responsibility of the public servants in relation to keeping absolute confidentiality on the content of the files. This obligation, in accordance with the provisions of the law, extends to the personnel of public or private organizations that may become aware of it in the exercise of their functions in support of the Mexican Institute of Industrial Property (IMPI). The only exceptions are information of an official nature or required by the judicial authority (art. 24 IPL).

It is also possible to request, either ex parte or ex officio, the adoption of the necessary measures to prevent unauthorized disclosure to third parties not involved in the dispute and to guarantee its confidentiality in any judicial or administrative proceeding related to this matter (art. 169 IPL), given that there is an express prohibition that no interested party may disclose or use the trade secret.

In summary, the confidential testing of this type of products could be framed within what is foreseen and possible by the same legal framework of intellectual property rights as a way to protect the owners of AI systems. However, it is important to note that this framework only operates in cases where there are public authority access obligations, in other words, certification mechanisms. The system of exceptions to access to information is only contemplated for a legal framework in which there are certification obligations, which in the case of AI systems should be related to their transparency.

4.2. Transparency and intellectual property in the transmission and adaptation of AI systems

From the technological point of view, the system must be transparent from the design phase and throughout its life cycle. The life cycle of the AI system consists of several phases[12], which may take place iteratively and not necessarily sequentially and involve various stakeholders, such as intellectual property rights-holders, service providers, importers, distributors and users. This means that, if the system is to be transparent and auditable in any of these phases, then whoever is in charge of it must have the technical information necessary to ensure this.

In other words, if such technical information is associated to a software, patent and/or secret, it must be transmitted together with the system and the necessary measures must be taken for its protection and to guarantee its updating according to its phase and life cycle. In Mexico, the LPI contemplates the possibility that the person exercising legal control of the secret may transmit it or authorize its use to a third party, under the obligation of not disclosing it (art. 165). Likewise, it is considered that in agreements where know-how, technical assistance, and provision of basic or detailed engineering are transmitted, confidentiality clauses may be established to protect industrial secrets as long as the aspects considered as confidential are specified.

12 According to the OECD recommendations, these phases are: i) design, data and modeling, which covers system planning and design, data collection and processing, and model building; ii) the verification and validation stage; iii) deployment; and finally, iv) operation and monitoring.

Therefore, compliance with the principle of transparency will depend on the role of each of the actors, as well as on the level of information that has been transmitted to them. The supplier, as the natural or legal person who develops an AI system or for whom the system is developed, plays a key role in fulfilling this obligation and particularly in providing the necessary documentation, implementing the code, carrying out traceability, use cases, appropriate specifications and so on.

The difference between the holder of the intellectual property rights over the system and the holder of the legal control of the industrial or commercial secret must be taken into account. At certain points in the life cycle this figure may coincide, but for the purposes of transparency depending on the type of protection, both figures are important given the capacity they may or may not have to authorize access to such information. For example, the provider may have developed the AI system or be the one for whom the system is developed. In the latter case, the relationship may have its cause in an employment or service contract, although it is also possible that the person is the owner of the AI system due to a transfer of intellectual property rights (software or patent). Whatever the cause for which the supplier becomes the owner of the rights, it does not mean that they are the person who introduces it on the market or places the system under their name or trademark.

In light of the above, it is possible that the supplier is not per se the owner of the rights over the system but the owner of the trademark or distinctive symbol that identifies it in the market. For transparency purposes, what is important is not the person who has ownership of the system but the person responsible for complying with the transparency obligation. However, it is not enough to be identified as such, but, in turn, they must have at their disposal the necessary information to be able to carry out the corresponding valuation or inspection and the necessary authorizations to do so.

In the latter case, it is of fundamental importance to determine who has legal control of confidential information, i.e., the person who can transmit or authorize the use of such information (article 65 of the Mexican IPL). This concept includes both the owner of the rights and of the information as well as the person who possesses it because it has been transferred or its use has been authorized. However, the agreements of transfer or authorization of use must be very clear in relation to the limits of this use and the possibility of complying or not with transparency obligations. On the other hand, a distinction must be made between those persons who have access to such information due to the position they hold and those who acquire the obligation to preserve it but cannot authorize its use to third parties, its transmission or delivery for the purpose of complying with the transparency obligation.

Generally speaking, all members of a system's value chain could be committed to a greater or lesser extent to complying with transparency obligations, with the duty to provide the necessary information. The guarantees for this to take place are the contracts entered into between the parties, as well as the adoption of the necessary protective measures to ensure the protection of business secrets. All the agents in the value chain are obliged to protect this information, given that if it is leaked, it immediately loses its secrecy.

Finally, the issue related to modifications or improvements to the system must be addressed. A distinction must be made between the fact that the system may continue to learn and improve after its introduction into the market or commissioning, or be intentionally subjected to a

substantial modification. In the latter case there could be an impact on the implementation, documentation and maintenance of the system, on the risk management associated with it or on the modification of the intended purpose for which it has been evaluated. In this case, the modification could only be carried out with the authorization of the holders of the intellectual property rights of the original system, having to undergo a new evaluation.

As it is software, in order to make any type of improvement or substantial change, the authorization of the copyright holder(s) must be obtained. As already mentioned above, among the powers of the owners of computer programs is that of authorizing or prohibiting the adaptation, arrangement or modification of the program, as well as the reproduction of the resulting program, the decompilation, the processes to reverse engineer a computer program and disassembly as well as the public communication of the program, including the making available to the public thereof (art. 106 LFDA). For these purposes, if the contract does not authorize these powers or does not provide for their transfer, these actions would infringe the right of the owners of the program.

In the proposed European regulation, there is an interesting delimitation that marks the extent to which it can be understood that the authorization of the owner of the system is necessary or not. For these purposes, a substantial modification is not considered to exist when the changes in the algorithm and its operation have been predetermined by the supplier and were taken into account at the time of the conformity assessment (recital 66). However, the modification of the system becomes difficult to prove if there is protection as an industrial or commercial secret. If there is no certification system, it would not be possible to prove the level of these modifications, how substantial they are or, at least, the sense of their implementation. In some cases, these may be minimal and even logical by taking as a starting point the same or similar algorithmic models. The only way to prove this distinction would be when there is a change in their purposes. In this case, the protection by way of secrecy could be undermined by not being able to prevent third parties from using it in a lawful manner as long as they obtain it by their own means.

5. Conclusions

Based on the foregoing, we could conclude that intellectual property rights can be a barrier or a driving mechanism for the development of AI systems. From the configuration of an AI public policy, it is necessary to devise a model for the protection of intellectual property rights over these systems that is consistent with a transparent regime that allows their auditing. Intellectual property rights should not become a barrier to the auditing, traceability and explainability of AI systems.

The level of transparency for reliable AI differs and depends not only on the information being transmitted but also on the context and the recipient of this information. In this regard, a distinction is made between transparency requirements aimed at meeting the expectations of users and consumers of these systems and those for auditing and/or certification purposes. When transparency requirements are aimed at meeting the expectations of users and consumers, it is not necessary to transmit information related to the source code or algorithm of the system, nor information associated with them. However, the situation is different when the purpose of transparency is to support requirements for certification and/or auditing of the systems. In this case, it is necessary to access the source code and associated information.

The value chain of AI systems is complex and involves multiple actors. The obligation of transparency remains with each of them; therefore, in order for each of the actors to comply with this obligation throughout the life cycle of the AI, there must be clear obligations in the contracts for the transmission and use of the systems that guarantee the provision of the information necessary to comply with this obligation, as well as guaranteeing respect for intellectual property rights.

AI systems may be protected by patents and copyrights such as software or industrial secrets. These forms of protection are not mutually exclusive and depend on national regulations. Given the particularities of each of these forms of protection, they impact differently on the intentional opacity of AI systems and on compliance with transparency requirements. Therefore, it is necessary to find a balance between transparency and property rights according to each of these forms of protection.

In the Mexican legal system, as in other countries in the Latin American region, the main mechanisms for protecting these systems are by means of copyright as software or as a trade secret. The legal framework of these concepts contemplates viable solutions that prevent intellectual property rights from becoming a barrier to the obligation of transparency of AI systems.

There are exceptions that make it possible to protect intellectual property rights and confidential business information or trade secrets of a natural or legal person, including the source code, provided that they are used in compliance with the confidentiality obligation of the competent national authorities in relation to information and data obtained in the exercise of their functions and activities to certify such systems. The non-existence of certification mechanisms, in principle, does not allow the requirements of these exceptions to be met.

6. References

AEPD (2018). El examen de aplicaciones (III): los términos y condiciones. [The application review (III): terms and conditions.] https://www.aepd.es/es/prensa-y-comunicacion/blog/el-examen-de-aplicaciones-iii-los-terminos-y-condiciones

Bengio, Yoshua (2018). Resistirse al monopolio de la investigación. [Resisting the research monopoly.] Artificial Intelligence, promises and threats. The UNESCO Courier. Julio-septiembre, (3), 18-20.

Bielan, Adam (2020). Opinión de la Comisión de Mercado Interior y Protección del consumidor para la Comisión de Asuntos Jurídicos sobre los derechos de propiedad intelectual para el desarrollo de las tecnologías relativas a la inteligencia artificial. [Opinion of the Committee on the Internal Market and Consumer Protection for the Committee on Legal Affairs on intellectual property rights for the development of technologies relating to artificial intelligence.] https://www.europarl.europa.eu/doceo/document/A-9-2020-0176_ES.html

British Embassy in Mexico (2018). Estrategia de IA en México: Aprovechando la Revolución de la IA. [AI Strategy in Mexico: Harnessing the AI Revolution.]

Burrell, Jennav (2016). How the machine 'thinks': Understanding opacity in machine learning algorithms. Big Data & Society, 3(1)-2053951715622512. https://journals.sagepub.com/doi/pdf/10.1177/2053951715622512

Castets-Renard, Celine (2020). The Intersection Between AI and IP: Conflict or Complementarity? Max Planck Institute for Innovation and Competition (IIC), 51, 141–143. https://doi.org/10.1007/s40319-020-00908-z

Cminds (2020). Agenda Nacional Mexicana de Inteligencia Artificial. México: Coalición IA2030Mx. [Mexican National Agenda for Artificial Intelligence. Mexico: IA2030Mx Coalition.]

European Commission (2019). Directrices Éticas para una IA Fiable. [Ethical Guidelines for Reliable AI.] https://ec.europa.eu/digital-single-market/en/high-level-expert-group-artificial-intelligence.

European Commission, (2020). Libro Blanco sobre la inteligencia artificial, un enfoque europeo orientado a la excelencia y la confianza. [White Paper on Artificial Intelligence, a European approach to excellence and trust.] https://op.europa.eu/es/publication-detail/-/publication/ac957f13-53c6-11ea-aece-01aa75ed71a1

Eticas Research and Consulting SL (2021), Guía de Auditoría Algorítmica. [Algorithmic Audit Guide.] Madrid: Spanish Data Protection Agency.

Felzmann, Heike, Fosch Villaronga, Eduard, Lutz Christoph and Tamò Larrieux, Aurelia (2020). Towards Transparency by Design for Artificial Intelligence. Science and Engineering Ethics, 26(6), 3333–3361. https://link.springer.com/content/pdf/10.1007/s11948-020-00276-4.pdf

Früh, Alfred (2021). Transparency in the Patent System – Artificial Intelligence and the Disclosure Requirement. En Pacud, Žaneta and Sikorski, Rafał (Ed.). Patents as an Incentive for Innovation. Kluwer Law International.

Hamon, R., Junklewitz, H., Sanchez, I. (2020). Robustness and Explainability of Artificial Intelligence - From technical to policy solutions. Publications Office of the European Union. DOI:10.2760/57493.

Herrera Triguero, Francisco (2019). Inteligencia computacional: sistemas inteligentes inspirados en la naturaleza. [Computational Intelligence: Intelligent Systems Inspired by Nature.] http://www.raing.es/sites/default/files/PUBLICACI%C3%93N%20FRANCISCO%20HERRERA.pdf

Hidalgo Pérez, Montse (2020). Leer las condiciones de tus 'apps' te puede llevar más tiempo que el Quijote. [Reading the terms and conditions of your apps can take you longer than Don Quixote.] El País. https://elpais.com/tecnologia/2020-06-23/leer-las-condiciones-de-tus-apps-te-puede-llevar-mas-tiempo-que-el-quijote.html

Hilty Reto, M., Hoffmann, Jörg and Scheuerer, Stefan (2020). Intellectual Property Justification for Artificial Intelligence. Max Planck Institute for Innovation and Competition Research Paper (02). https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3539406

Kaminski, Margot E. (2019). The right to explanation, explained. Berkeley Technology Law Journal (34). https://scholar.law.colorado.edu/articles/1227

Mökander, Jakob and Floridi, Luciano (2021). Ethics Based Auditing to Develop Trustworthy AI. Minds and Machines. https://doi.org/10.1007/s11023-021-09557-8

Federal Copyright Law. New Law published in the Official Gazette of the Federation on December 24, 1996. Current text, last amendment published DOF 01-07-2020.

Federal Law of Transparency and Access to Public Information. New Law published in the Official Gazette of the Federation on May 9, 2016. Current text, last amendment published DOF 20-05-2021.

Federal Law for the Protection of Industrial Property. Text in force. New Law published in the Official Gazette of the Federation on July 1, 2020.

Free Trade Agreement between Mexico, United States and Canada, effective as of July 1, 2020.

The Economist Intelligence Unit (EIU) and the ABB company (2018). Índice de Preparación para la automatización. [Automation Readiness Index.]

OECD (2019). Recommendation of the Council on Artificial Intelligence, OECD/LEGAL/0449. https://legalinstruments.oecd.org› api › print

Oliver Ramírez, Nuria María (2018). Inteligencia artificial: Ficción, realidad y... Sueños. [Artificial Intelligence: Fiction, reality and... Dreams.] http://www.raing.es/sites/default/files/TOMA%20DE%20POSESI%C3%93N%20NURIA%20OLIVER%2011.12.18.pdf

Oxford Insights (2021). Government AI Readiness Index 2020. Canada's International Development Research Centre (IDRC). https://www.oxfordinsights.com/government-ai-readiness-index-2020

European Parliament and Council (2021). Propuesta de Reglamento por el que se establecen normas armonizadas en materia de Inteligencia Artificial (Ley de Inteligencia Artificial) y se modifican determinados actos legislativos de la Unión, 2021/0106(COD). [Proposal for a Regulation laying down harmonized rules in the field of Artificial Intelligence (Artificial Intelligence Act) and amending certain legislative acts of the Union, 2021/0106(COD).] https://eur-lex.europa.eu/legal-content/ES/TXT/?uri=COM:2021:206:FIN

Paz Hermosilla, María; Garrido, Romina and Ioewe, Daniel, (2020). Transparencia y responsabilidad algorítmica para la inteligencia artificial. [Transparency and algorithmic accountability for artificial intelligence.]

Plaza, Javier (2019). Aspectos legales del Big Data y la Inteligencia Artificial. Big Data e Inteligencia Artificial: Una visión económica y legal de estas herramientas disruptivas. [Legal aspects of Big Data and Artificial Intelligence. Big Data and Artificial Intelligence: An economic and legal view of these disruptive tools.]

Qiang, Yang (2018). La cuarta revolución. Inteligencia artificial. Promesas y amenazas. [The fourth revolution. Artificial Intelligence. Promises and threats.] The Unesco Courier.

Unesco (2020). Primera versión del proyecto de recomendación sobre la ética de la inteligencia artificial [First version of the draft recommendation on the ethics of artificial intelligence.] SHS/BIO/AHEG-AI/2020/4 REV.2. https://unesdoc.unesco.org/ark:/48223/pf0000373434_spa

Verheyen, Sabine (2020). Opinión de la Comisión de Cultura y Educación para la Comisión de Asuntos Jurídicos sobre los derechos de propiedad intelectual en el desarrollo de tecnologías de inteligencia artificial, [Opinion of the Committee on Culture and Education for the Committee on Legal Affairs on intellectual property rights in the development of artificial intelligence technologies.] 3/09/2020 (2020/2015(INI). https://www.europarl.europa.eu/doceo/document/A-9-2020-0176_ES.html

WIPO (2019). WIPO Technology Trends 2019: Artificial Intelligence. https://www.wipo.int/edocs/pubdocs/en/wipo_pub_1055.pdf